From: Andrew Lewman, Executive Director
To: the tor community
Date: April 10, 2011

This report documents progress in March 2011.

New releases, new hires, new funding

New Hires

Contracted Tomas Touceda to fix bugs and develop new features for the Tor graphical controller, Vidalia.

New Funding

Tor receives an anonymous donation to improve hidden services performance, reliability, and general bug fixes.

New Releases

1. On March 9th we released updated Tor Browser Bundles for Microsoft Windows, Apple OS X, and GNU/Linux operating systems. All of the Tor Browser Bundles have been updated with Firefox 3.6.15 and the alpha bundles for Mac OS X and Linux have also been updated with Tor 0.2.2.23-alpha.

```
Windows bundles 1.3.20: Released 2011-03-07
Update Firefox to 3.6.15

Linux bundles 1.1.5: Released 2011-03-09
Update Tor to 0.2.2.23-alpha
Update Firefox to 3.6.15
Update NoScript to 2.0.9.8
Update HTTPS-Everywhere to 0.9.9.development.3

OS X bundle 1.0.13: Released 2011-03-09
Update Tor to 0.2.2.23-alpha
Update Firefox to 3.6.15, and use the Mozilla version until I get it to build on OS X 10.6 (Snow L
Update NoScript to 2.0.9.8
Update HTTPS-Everywhere to 0.9.9.development.3
```

2. On March 8th, we released the latest in the tor -alpha series, 0.2.2.23. Tor 0.2.2.23-alpha lets relays record their bandwidth history so when they restart they don't lose their bandwidth

capacity estimate. This release also fixes a diverse set of user-facing bugs, ranging from relays overrunning their rate limiting to clients falsely warning about clock skew to bridge descriptor leaks by our bridge directory authority.

```
Changes in version 0.2.2.23-alpha - 2011-03-08

  o Major bugfixes:
    - Stop sending a CLOCK_SKEW controller status event whenever
      we fetch directory information from a relay that has a wrong clock.
      Instead, only inform the controller when it’s a trusted authority
      that claims our clock is wrong. Bugfix on 0.1.2.6-alpha; fixes
      the rest of bug 1074.
    - Fix an assert in parsing router descriptors containing IPv6
      addresses. This one took down the directory authorities when
      somebody tried some experimental code. Bugfix on 0.2.1.3-alpha.
    - Make the bridge directory authority refuse to answer directory
      requests for "all" descriptors. It used to include bridge
      descriptors in its answer, which was a major information leak.
      Found by "piebeer". Bugfix on 0.2.0.3-alpha.
    - If relays set RelayBandwidthBurst but not RelayBandwidthRate,
      Tor would ignore their RelayBandwidthBurst setting,
      potentially using more bandwidth than expected. Bugfix on
      0.2.0.1-alpha. Reported by Paul Wouters. Fixes bug 2470.
    - Ignore and warn if the user mistakenly sets "PublishServerDescriptor
      hidserv" in her torrc. The ’hidserv’ argument never controlled
      publication of hidden service descriptors. Bugfix on 0.2.0.1-alpha.

  o Major features:
    - Relays now save observed peak bandwidth throughput rates to their
      state file (along with total usage, which was already saved)
      so that they can determine their correct estimated bandwidth on
      restart. Resolves bug 1863, where Tor relays would reset their
      estimated bandwidth to 0 after restarting.
    - Directory authorities now take changes in router IP address and
      ORPort into account when determining router stability. Previously,
      if a router changed its IP or ORPort, the authorities would not
      treat it as having any downtime for the purposes of stability
      calculation, whereas clients would experience downtime since the
      change could take a while to propagate to them. Resolves issue 1035.
    - Enable Address Space Layout Randomization (ASLR) and Data Execution
      Prevention (DEP) by default on Windows to make it harder for
      attackers to exploit vulnerabilities. Patch from John Brooks.

  o Minor bugfixes (on 0.2.1.x and earlier):
    - Fix a rare crash bug that could occur when a client was configured
      with a large number of bridges. Fixes bug 2629; bugfix on
      0.2.1.2-alpha. Bugfix by trac user "shitlei".
    - Avoid a double mark-for-free warning when failing to attach a
      transparent proxy connection. Bugfix on 0.1.2.1-alpha. Fixes
      bug 2279.
    - Correctly detect failure to allocate an OpenSSL BIO. Fixes bug 2378;
```

```
      found by "cypherpunks". This bug was introduced before the first
      Tor release, in svn commit r110.
    - Country codes aren't supported in EntryNodes until 0.2.3.x, so
      don't mention them in the manpage. Fixes bug 2450; issue
      spotted by keb and G-Lo.
    - Fix a bug in bandwidth history state parsing that could have been
      triggered if a future version of Tor ever changed the timing
      granularity at which bandwidth history is measured. Bugfix on
      Tor 0.1.1.11-alpha.
    - When a relay decides that its DNS is too broken for it to serve
      as an exit server, it advertised itself as a non-exit, but
      continued to act as an exit. This could create accidental
      partitioning opportunities for users. Instead, if a relay is
      going to advertise reject *:* as its exit policy, it should
      really act with exit policy "reject *:*". Fixes bug 2366.
      Bugfix on Tor 0.1.2.5-alpha. Bugfix by user "postman" on trac.
    - In the special case where you configure a public exit relay as your
      bridge, Tor would be willing to use that exit relay as the last
      hop in your circuit as well. Now we fail that circuit instead.
      Bugfix on 0.2.0.12-alpha. Fixes bug 2403. Reported by "piebeer".
    - Fix a bug with our locking implementation on Windows that couldn't
      correctly detect when a file was already locked. Fixes bug 2504,
      bugfix on 0.2.1.6-alpha.
    - Fix IPv6-related connect() failures on some platforms (BSD, OS X).
      Bugfix on 0.2.0.3-alpha; fixes first part of bug 2660. Patch by
      "piebeer".
    - Set target port in get_interface_address6() correctly. Bugfix
      on 0.1.1.4-alpha and 0.2.0.3-alpha; fixes second part of bug 2660.
    - Directory authorities are now more robust to hops back in time
      when calculating router stability. Previously, if a run of uptime
      or downtime appeared to be negative, the calculation could give
      incorrect results. Bugfix on 0.2.0.6-alpha; noticed when fixing
      bug 1035.
    - Fix an assert that got triggered when using the TestingTorNetwork
      configuration option and then issuing a GETINFO config-text control
      command. Fixes bug 2250; bugfix on 0.2.1.2-alpha.

  o Minor bugfixes (on 0.2.2.x):
    - Clients should not weight BadExit nodes as Exits in their node
      selection. Similarly, directory authorities should not count BadExit
      bandwidth as Exit bandwidth when computing bandwidth-weights.
      Bugfix on 0.2.2.10-alpha; fixes bug 2203.
    - Correctly clear our dir_read/dir_write history when there is an
      error parsing any bw history value from the state file. Bugfix on
      Tor 0.2.2.15-alpha.
    - Resolve a bug in verifying signatures of directory objects
      with digests longer than SHA1. Bugfix on 0.2.2.20-alpha.
      Fixes bug 2409. Found by "piebeer".
    - Bridge authorities no longer crash on SIGHUP when they try to
      publish their relay descriptor to themselves. Fixes bug 2572. Bugfix
      on 0.2.2.22-alpha.
  o Minor features:
    - Log less aggressively about circuit timeout changes, and improve
      some other circuit timeout messages. Resolves bug 2004.
    - Log a little more clearly about the times at which we're no longer
      accepting new connections. Resolves bug 2181.
    - Reject attempts at the client side to open connections to private
      IP addresses (like 127.0.0.1, 10.0.0.1, and so on) with
      a randomly chosen exit node. Attempts to do so are always
      ill-defined, generally prevented by exit policies, and usually
      in error. This will also help to detect loops in transparent
      proxy configurations. You can disable this feature by setting
      "ClientRejectInternalAddresses 0" in your torrc.
    - Always treat failure to allocate an RSA key as an unrecoverable
      allocation error.
    - Update to the March 1 2011 Maxmind GeoLite Country database.

  o Minor features (log subsystem):
    - Add documentation for configuring logging at different severities in
      different log domains. We've had this feature since 0.2.1.1-alpha,
      but for some reason it never made it into the manpage. Fixes
      bug 2215.
    - Make it simpler to specify "All log domains except for A and B".
      Previously you needed to say "[*,˜A,˜B]". Now you can just say
      "[˜A,˜B]".
    - Add a "LogMessageDomains 1" option to include the domains of log
      messages along with the messages. Without this, there's no way
      to use log domains without reading the source or doing a lot
      of guessing.

  o Packaging changes:
    - Stop shipping the Tor specs files and development proposal documents
      in the tarball. They are now in a separate git repository at
      git://git.torproject.org/torspec.git
```

3. On March 24th, all of the Tor Browser Bundles have been updated with Firefox 3.6.16 and the alpha bundles for Mac OS X and Linux have also been updated to use Libevent 2, as well as a number of extension updates. The changelogs are below.

```
Windows bundles 1.3.21: Released 2011-03-23
Update Firefox to 3.6.16
Update HTTPS-Everywhere to 0.9.9.development.4

Linux bundles 1.1.6: Released 2011-03-23
Update Firefox to 3.6.16
Update Libevent to 2.0.10-stable
Update NoScript to 2.0.9.9
Update HTTPS-Everywhere to 0.9.9.development.4
Update BetterPrivacy to 1.49

OS X bundle 1.0.14: Released 2011-03-23
```

```
Update Firefox to 3.6.16
Update Libevent to 2.0.10-stable
Update NoScript to 2.0.9.9
Update HTTPS-Everywhere to 0.9.9.development.4
Update BetterPrivacy to 1.49
```

4. On March 27th, we have new Firefox 4 Tor Browser Bundles available for OS X. They come in 64- and 32-bit versions, and one important fix for 10.6 64-bit users is that Firefox no longer crashes on initial startup. These are alpha, but they are going to be a permanent addition to the Tor Browser Bundle family and will be maintained from now on. These have thus far only been tested on Snow Leopard, but the 32-bit bundle ought to work on Leopard.

```
Tor Browser Bundle (2.2.23-1) alpha; suite=osx
Create new bundles for Firefox 4, both i386 and x86_64 (closes: #2140)
Update Tor to 0.2.2.23-alpha
Update Torbutton to 1.3.2-alpha
Update OpenSSL to 1.0.0d
Update HTTPS-Everywhere to 0.9.9.development.4
Update NoScript to 2.0.9.9
Update BetterPrivacy to 1.49
```

5. On March 31st, we released bridge by default bundles. These were previously released as a technology preview but we're going to bring them back on a consistent basis. We have an updated bridge by default Vidalia bundle for Windows available with Tor 0.2.2.23-alpha.

6. On March 31st, we now have Firefox 4 bundles available for GNU/Linux.

```
Tor Browser Bundle (2.2.23-1) alpha; suite=linux
Create new bundles for Firefox 4, both i386 and x86_64
Update Tor to 0.2.2.23-alpha
Update Torbutton to 1.3.2-alpha
Update OpenSSL to 1.0.0d
Update HTTPS-Everywhere to 0.9.9.development.4
Update NoScript to 2.0.9.9
Update BetterPrivacy to 1.49
```

7. On March 21st, we released the latest in the torbutton alpha branch, version 1.3.2. It fixes a few outstanding bugs and better supports Firefox 4.

```
  * bug 1624: Use nsIDOMCrypto::logout() instead of the SSLv2 pref hack
  * bug 1999: Disable tor:// urls by default
  * bug 1968: Reset window.name on tor toggle
  * bug 2148: Make refspoofing more uniform
  * bug 2359: Fix XHTML DTD errors on FF4
  * bugs 2465+2421: Fix javascript hook exceptions+issues in FF4.0
  * bug 2458: Opt out of Firefox addon usage pings
  * bug 2377: Limit the Google captcha cookies copied between google TLDs
  * bug 2491: Clean up checks for when to jar protected cookies
  * bug 1110: Add popup to ask if we should spoof English Accept: headers
  * misc: Remove a noisy FF2 nsICookieManager2 fallback check.
```

Design, develop, and implement enhancements that make Tor a better tool for users in censored countries.

1. Jacob did research into and wrote up his analysis of suspicious SSL certificates from Comodo, `https://blog.torproject.org/blog/detecting-certificate-authority-compromises-and-web-brow`
2. Mike wrote a client for EFF's SSL Observatory to provide users with the ability to opt-in to submitting "strange" SSL certificates.
3. Mike helped write a paper for the W3C Workshop on Identity in the Browser, `http://www.w3.org/2011/identity-ws/Overview.html`.
4. Karsten refactored metrics-db and metrics-web by moving a lot of code from metrics-db to metrics-web (2627). metrics-db is now the tool for collecting and sanitizing metrics data, and metrics-web is the metrics website including the database schema and database import. This separation was necessary to enable people to run their own metrics-web without having to run their own metrics-db.
5. Karsten improved detection of stale bridge descriptor tarballs from Tonga by comparing descriptor publication times to tarball modification times (`https://trac.torproject.org/projects/tor/ticket/2570`).
6. Karsten extended BridgeDB to dump assignments to disk (`https://trac.torproject.org/projects/tor/ticket/2372`), wrote a script to convert old BridgeDB logs into assignment files, and extended metrics-db to sanitize these files. The files are now on the metrics website.
7. Karsten provided bridge usage data in a format that researchers can analyze much easier than the original data (`https://trac.torproject.org/projects/tor/ticket/2680`).
8. Karsten created a Thematic Mapping API prototype as a fancy example for visualizing Tor data (`https://trac.torproject.org/projects/tor/ticket/2762`).

Architecture and technical design docs for Tor enhancements related to blocking-resistance.

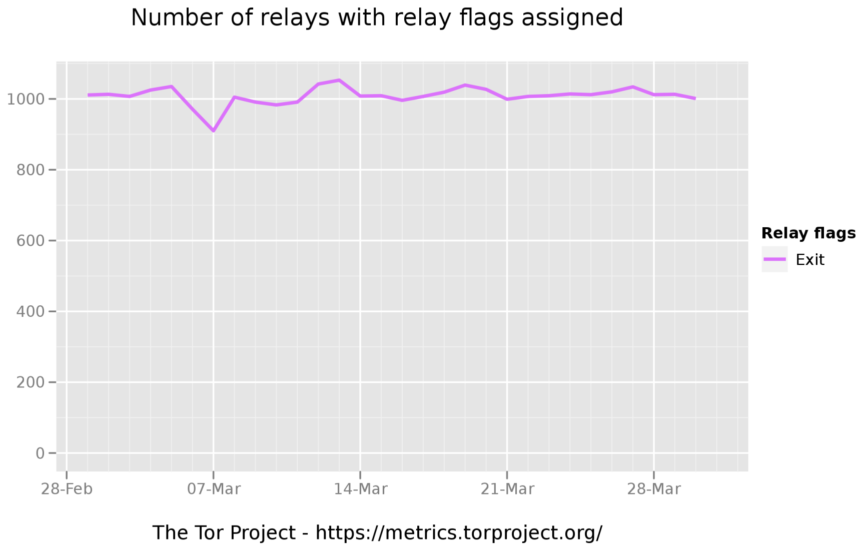
1. Karsten wrote a roadmap for the various metrics products or products that have a metrics part: metrics-web, metrics-db, ExoneraTor, VisiTor, BridgeDB, Torperf, Tor websites, bandwidth scanners, TorDNSEL, and Tor.

Hide Tor's network signature.

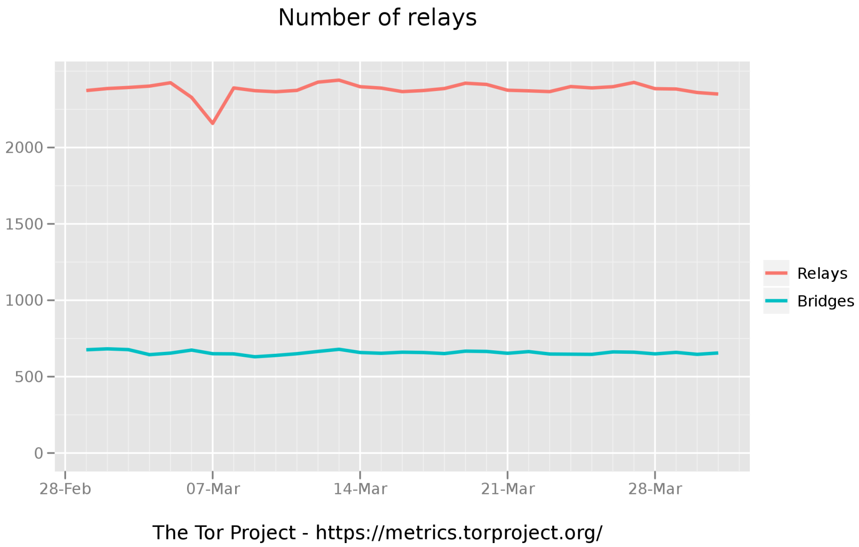
1. The pluggable transport protocol is an official proposal, number 180. `https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/180-pluggable-transport.txt`
2. Design updates to the TLS cert and parameter normalizations proposal, number 179, `https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/179-TLS-cert-and-parameter-norma`
   `txt`.

Grow the Tor network and user base. Outreach.

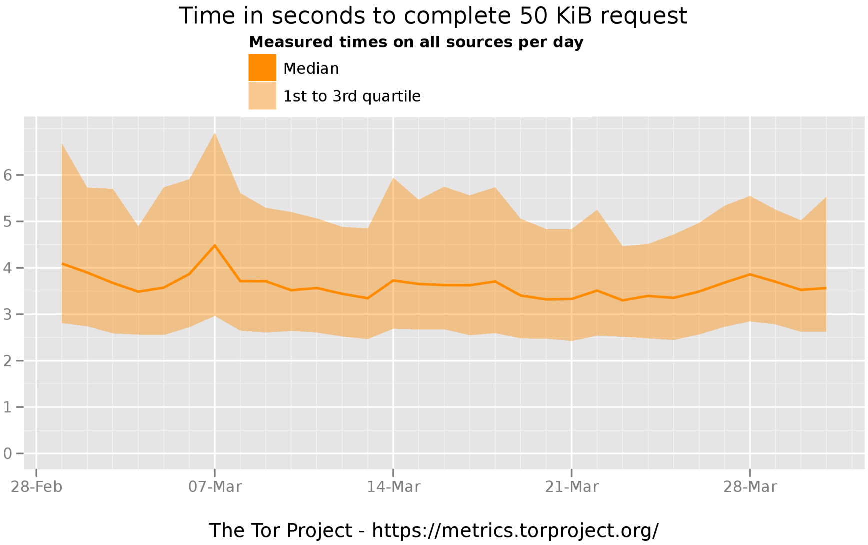
Measures of the Tor Network



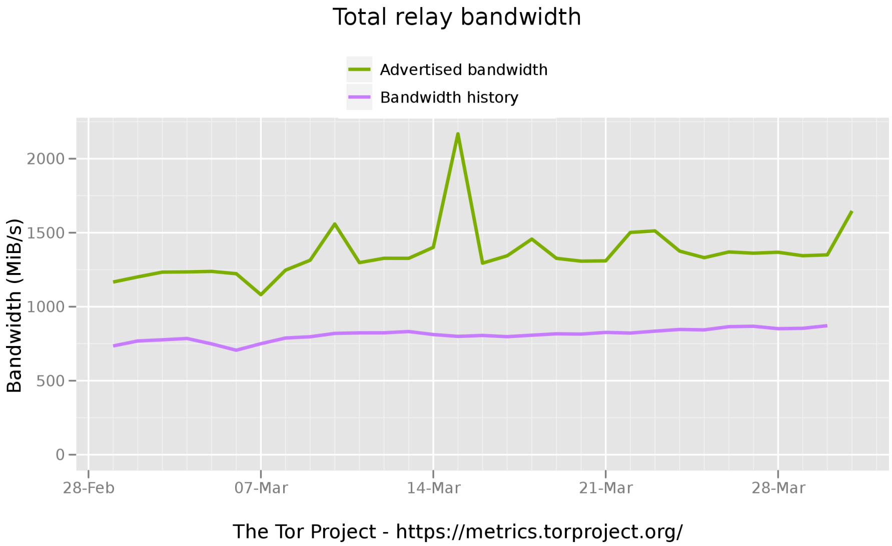
This graph shows the total quantity of exit relays in March 2011. We seem to have kept most of our relays since the bump due to Tunisia and Egypt.



This graph shows the total quantity of relays and the total quantity of bridges in March 2011. We seem to have kept most of our relays since the bump due to Tunisia and Egypt.



This graphs shows how many seconds it took to complete a 50KB download from a standard Tor client. This is an average of all measurements from servers located in Illinois, Massachusetts, and Sweden. Performance remains relatively steady at just under 4 seconds.



This graph shows the total available bandwidth available to clients and how much was actually used throughout the month. The steady-state of relays creates almost 1.6GBps (12.8 Gbps) of bandwidth available.

Outreach and Advocacy

1. We held a Privacy and Security Workshop at the University of London School of Oriental and African studies, `https://blog.torproject.org/blog/london-internet-security-privacy-workshop`.

2. At LibrePlanet 2011, Tor received the 2010 FSF/GNU Project Award for Project of Social Benefit. https://blog.torproject.org/blog/tor-project-receives-fsf-award.

3. Roger took a lengthy trip to Taiwan. Spoke at OSDC'11 among other locales. His trip report is at https://blog.torproject.org/blog/trip-report-taipei.

4. Andrew was interviewed by the Washington Post about US firms helping censor the Internet, http://www.washingtonpost.com/wpdyn/content/article/2011/03/09/AR2011030905157_pf.html.

5. Wendy attended ICANN in San Francisco.

6. Andrew met with Gunilla Carlsson, the Swedish Minister of Foreign Development, and staff to discuss Tor, digital democracy, and democratic digitalization, http://www.nyteknik.se/nyheter/it_telekom/internet/article3123594.ece

7. Roger and Robert met ISI to discuss Tor and network simulation, http://www3.isi.edu/home.

8. Andrew was interviewed by Businessweek about social networking, http://www.businessweek.com/magazine/content/11_13/b4221043353206.htm

9. Erinn gave a talk at PMF (mathematički fakultet) Zagreb about Tor.

10. Erinn met with a Zagreb hackerspace, http://www.mi2.hr/, to talk about Tor.

11. Andrew was interviewed by The Telegraph to understand what's going on with Tor and Iran, http://www.telegraph.co.uk/news/worldnews/middleeast/iran/8388484/Iran-cracks-down-on-web
html

12. Jacob gave a speech at the Royal Military College of Canada, http://www.rmc.ca/

13. Andrew was featured by CNN on The Situation Room with Wolf Blitzer about US companies helping censor the Internet, http://edition.cnn.com/CNN/Programs/situation.room/

14. Nick gave a speech at the 4th Usenix Workshop on Large-scale Exploits and Emergent Threats, http://www.usenix.org/events/leet11/.

15. Tor was a finalist in the Index on Censorship New Media award, http://www.indexoncensorship.org/2011/03/free-expression-awards-2011-new-media/

16. Andrew and Karen talked to the US Senate Committee on Foreign Relations about Tor, online anonymity and privacy.

Preconfigured privacy (circumvention) bundles for USB or LiveCD.

1. TAILS nears a 0.7 release through testing of Release Candidates, http://tails.boum.org/.

2. See the "New Releases" section above for the various Tor Browser Bundles released.

Bridge relay and bridge authority work.

1. Torservers.net receives $10,000 to operate more bridges to support people in heavily censored areas, https://www.torservers.net/wiki/press.
2. Robert and Christian fixed a few bugs and integrated some features into the Bridge Authority codebase, https://gitweb.torproject.org/bridgedb.git/shortlog.

Scalability, load balancing, directory overhead, efficiency.

1. Karsten and Mike started to design a tech report using the torperf to monitor the network through a series of experiments, the ticket list for which is here: https://trac.torproject.org/projects/tor/ticket/2769.
2. Mike did a quick review of Ian, Damon, et al's paper on their flow control and simulator work: https://lists.torproject.org/pipermail/tor-dev/2011-March/002539.html
3. Sebastian worked on libevent and Tor, to make it possible to compile them with clang with warnings. While doing so he started porting some of Tor's configure options to libevent, and fixed a few minor bugs that clang exposed.
4. Sebastian and Tomas converted Vidalia's repository from svn to git. This will allow for more distributed patches and branches.
5. Karsten reviewed and merged Mike's patch for Torperf's consolidate_stats script (https://trac.torproject.org/projects/tor/ticket/2672).
6. Karsten started writing a paper/report on Torperf and the bwscanners together with Mike (https://trac.torproject.org/projects/tor/ticket/2769). Prepared new graphs (https://trac.torproject.org/projects/tor/ticket/2772, https://trac.torproject.org/projects/tor/ticket/2394) and set up Torperfs to determine the optimal circuit build timeout cutoff (https://trac.torproject.org/projects/tor/ticket/2770).
7. Nick updates the core tor specification to include the optimistic data protocol, https://gitweb.torproject.org/torspec.git/commitdiff/ef0bff2ff3c14934a6cd056d8a9d03151741c675

Incentives work.

Nothing to report.

More reliable (e.g. split) download mechanism.

Nothing to report.

Footprints from Tor Browser Bundle.

Nothing to report.

Translation work, ultimately a browser-based approach.

1. Runa did a bundle of work on translations, coordinating translators, and updating our various products with translations. The highlights are:

```
- updated translations from transifex (in
translation/trunk/projects/manpages/po: .tx af       ak am arn ast az
be bg bn bn_IN ca cs csb cy dz el eo eu fil fur ga gl gu gun ha he
hi hr ht hu is kn kw lb ln lo lt lv mg   mi mk ml mn mr ms mt nap nb
ne nl nn nso oc pa pap pms ps pt    pt_BR ro sco son su sw ta te tg th
ti tk uk ur ve vi wa zh_CN zh_HK zh_TW zu)
- updated translations from transifex for orbot (in
translation/trunk/projects/orbot/po:     .tx af ak am arn ast az be
bg bn bn_IN cs csb dz el eo et eu    fil fur ga gl gu gun ha he hi hr
ht id kn kw lb ln lo lt lv mg mi ml mn mr ms mt my nap ne nn nso
oc pa pap pms ps pt_BR    ro sco son sw ta te tg th ti tk uk ve vi wa
zh_HK zh_TW zu)
- updated translations from transifex for torbutton (in
translation/trunk/projects/torbutton/po: .tx af ak am arn ast be bg
bn bn_IN csb cy dz eo eu fil fur ga gl gun ha he hi ht    hu is kn kw
lb ln lo lt lv mg mi ml mn mr ms mt nap ne nn nso   oc pa pap pms ps
sco son su sw ta te tg th ti tk uk ur ve wa zh_HK zu)
- updated translations from transifex for torbutton-alpha (in
translation/trunk/projects/torbutton-alpha/po: .tx af ak am   arn
ast az be bg bn bn_IN csb cy dz eo eu fil fur ga gl gun     ha he ht
hu is kn kw lb ln lo lt lv mg mi mk ml mn mr ms mt nap ne nn nso
oc pa pap pms ps sco son su sw ta te tg ti tk    ur ve wa zh_HK zu)
- updated translations from transifex for torcheck (in
translation/trunk/projects/torcheck/po: .tx af ak am arn ast  az bg
bn_IN csb de_CH dz eo eu fil fur ga gu gun ha he hr ht    is kn lb ln
lo lt lv mg mi ml mn mr ms mt nah nap ne nn nso     oc pa pap pms ps
sco son su ta te tg ti tk ur ve zh_HK zu)
- updated translations from transifex for the website (in
translation/trunk/projects/website/po: .tx zh_CN/about)
- updated translations for vidalia (in vidalia/trunk/src/vidalia/i18n/po:
.tx af ak am arn ast az be   bg bn bn_IN bo br bs ca csb cy de_CH de_DE
dz et eu fil fo      fur fy ga gl gun ha hi hr ht hy is jv ka km kn
ko ku kw ky lb   ln lo lt lv mg mi mk ml mn mr ms mt nah nap ne nn nso
oc or    pa pap pms ps sco sk so son st su sw ta te tg th ti tk uk ur
ve vi wa wo zh_HK zu)
- updated translations for vidaliahelp (in
vidalia/trunk/src/vidalia/help/content/po: .tx af ak am arn ast az be
bg bn bn_IN ca cs csb cy dz el eo et eu fil fur ga    gl gu gun ha he
hi hr ht hu id is kn kw lb ln lo lt lv mg mi  mk ml mn mr ms mt nap
nb ne nl nn nso oc pa pap pms ps pt ro    sco son su sw ta te tg th ti
tk tr uk ur ve vi wa zh_HK zh_TW zu)
- updated translations for vidalia installer (in
vidalia/trunk/pkg/win32/po: .tx af ak am arn ast bg bn_IN csb  cy
de_CH dz eo eu fil fur ga gl gu gun ha hi hr ht hu is kn    lb ln lo
lt lv mg mi mk ml mn mr ms mt nah nap ne nn nso oc pa pap pms ps
pt_BR sco son su sw ta te tg ti tk ur ve zh_HK zu)
```

```
- translations for vidaliahelp as html files (in
vidalia/trunk/src/vidalia/help/content: . my zh_CN)
```